THE ASSISTANT COMMISSIONER OF PATENTS
Washington, D.C. 20231

DOCKET NUMBER: **AUS000060US1**
MARCH 20, 2000

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventor: **RABINDRANATH DUTTA**

For: **THIRD PARTY CONTRACT DEPOSITORY FOR E-COMMERCE TRANSACTIONS**

Enclosed are:

X Patent Specification and Executed Declaration

X 11 sheets of drawing(s).

X An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).

__ A certified copy of a __ application.

__ Information Disclosure Statement, PTO 1449 and copies of references.

The filing fee has been calculated as shown below:

For	Number Filed	Number Extra	Rate	Fee
Basic Fee				$690.00
Total Claims	18 - 20	0	x 18 =	$
Indep. Claims	5 - 3	2	x 78 =	$156.00
0 MULTIPLE DEPENDENT CLAIM PRESENTED			x 270 =	$
			TOTAL	$846.00

X Please charge IBM Corporation Deposit Account No. 09-0447 in the amount of $846.00. A duplicate copy of this sheet is enclosed.

X The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to IBM Corporation Deposit Account 09-0447. A duplicate copy of this sheet is enclosed.

X Any additional filing fees required under 37 CFR §1.16.

X Any patent application processing fees under 37 CFR §1.17.

Respectfully submitted,

By _____

Eustace P. Isidore
Registered with Limited Recognition - *see attached*
FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP
Suite 350 Lakewood on the Park
7600B North Capital of Texas Highway
Austin, Texas 78731
Telephone (512) 343-6116

THIRD PARTY CONTRACT DEPOSITORY FOR E-COMMERCE TRANSACTIONS

The present invention is related to the subject-matter of the following commonly assigned, co-pending United States Patent Application, Serial No. _____ (Docket No. AUS000060US2) entitled "Method and System for Maintaining Confidentiality of Personal Information During E-commerce Transactions," filed concurrently herewith.

BACKGROUND OF THE INVENTION

1. Technical Field:

The present invention relates in general to commercial transactions and in particular to commercial transactions on the Internet. Still more particularly, the present invention relates to a method, system and program for improving the integrity of documents created during commercial transactions on the Internet.

2. Description of the Related Art:

Internet commerce or E-commerce, as it is commonly referred to in the industry, is quickly becoming a preferred method of conducting commercial transactions. Many traditional and non-traditional businesses have realized the vast potential of conducting business on the Internet and have established web sites by which potential customers or clients may remotely access their respective information or products. This merging of business with the electronic medium of the Internet has

thus resulted in an increase in commercial and personal transactions.

E-commerce transactions may be either point-to-point/bipartite (i.e., an individual communicating directly with another individual or a business web site) or multi-point (i.e., many individuals transacting with each other, as in a swap room, or with on-line auctions, for example). Typically, a web server provides the background within which these E-commerce transactions take place.

Currently, most E-commerce transactions are bipartite and occur between a merchant and a buyer. The merchant is represented online by a web site located on a web server and accessible via a universal resource locator (URL) or web address. The buyer connects to the Internet via one of several known means of connecting to the Internet and accesses the merchant's web site. The merchant and the buyer enter into a transaction within the web server, which is recorded in electronic form on the web server as an agreement (or contract). Thus, the contract is typically stored in the web server of the merchant. A buyer may be provided with the opportunity to print the contract prior to terminating the connection to the web site.

As in traditional commercial transactions, disputes often arise about the actual terms (price, quantity, freight charges, etc.) of a transaction subsequent to the creation of the contract. In the traditional arena, contracts are typically in written form and at least one party has signed the original contract document verifying its authenticity. The terms, as written in this document

are difficult, if not impossible, to manipulate without being noticeable once the signature has been affixed to the page.

In the electronic medium of the Internet, electronic documents are generated, which are typically stored on the merchant's web server and are easily modifiable. The electronic nature of the document allows anyone with access to the web server to modify the terms of the original agreement. There is thus an inherent uncertainty in the validity of electronic documents. It is therefore difficult for the buyer or a third party arbitrator to determine the authenticity of the documents when a dispute arises.

Several prior art patents have taught methods for ensuring authenticity of communications/documents on the Internet with the use of digital signatures. U.S. Patent No. 5,949,876 discloses a system and method for secure transaction management for insuring that information is accessed and utilized only in an authorized way. U.S. Patent No. 5,850,442 teaches the use of public key infrastructure (i.e., smart token technology) to secure electronic transactions. A third party is utilized to register an application which is held and made accessible to the recipient after signature verification/ authentication using a smart token.

Both of these patents use a digital signature, which may be provided to both the buyer and merchant. Use of digital signatures, however, has not been adopted widely by the Internet community, particularly due to associated costs and other logistical concerns, such as the

complexity involved in creating the digital signatures and revoking lost or compromised digital signatures.

Another method, which utilizes a third party, has been proposed by United Parcel Services (UPS) OnLine Courier®. This method essentially allows the delivery of secure e-mail via the UPS as a depository third party. The sender sends a document using UPS OnLine Courier. The document is securely uploaded to the secure UPS OnLine Courier server, which sends an e-mail notification to the recipient that there is a document delivery for him. The recipient uses the URL provided in the e-mail to download the document from the secure UPS OnLine Courier server via a Web browser. As an option, the sender may specify that the recipient may only download the file if he has provided a password to the UPS OnLine Courier server, insuring the sender that only the intended recipient may open the document.

Another problem encountered during E-commerce transactions is the loss of or low levels of privacy with respect to distribution of personal information (name, address, email address, etc.) of a buyer. Buyers are usually required to enter personal information into the merchant's web site when conducting a transaction. E-bay, for example, provides multi-point E-commerce transactions; however, E-bay displays the personal information of each visitor who transacts on the site and does not provide for any anonymity/confidentiality. Occasionally, merchants subject their buyers to unsolicited e-mails (referred to as "junk mail") or physical mail, which advertise products of the merchant or another entity to which the merchant has forwarded the buyer's personal information. Also, the buyer may wish to

withhold his personal information from the merchant for other reasons.

In some instances, a seller may wish to have his personal information kept private. Currently, anyone may access personal information (such as name and address) about the owner of a web site (i.e., find out to whom a web server belongs) by looking up the domain name in one of the several server databases publicly available through issuers of Internet domain names and affiliated groups.

Prior art attempts to handle this problem includes U.S. Patent Nos. 5,692,982 and 5,553,145, which disclose the use of a third (trusted) party to transmit an encrypted message from one party to a second party, whereby the identity of the communicating parties may be kept secret (from the third party). A receipt is sent to the sending party when the communication is received by the receiving party. The method also uses a digital signature where each party has a secret signing key and matching public verification key for sending and accessing the content of the communication. Other related patents include U.S. Patent 5,666,420 which utilizes a third party to communicate if a first attempt to communicate directly fails. Chat rooms allow use of pseudonyms during internet communications but do not extend into the internet-based commercial transactions in the context of exchange of financial information.

None of the prior art methods discloses an efficient and globally available/applicable method for ensuring the integrity of electronic documents created during a commercial transaction conducted over the Internet. The

present invention thus recognizes that it would be desirable to provide a method and system for providing this functionality (i.e., ensuring the integrity of electronic documents) in an efficient and globally applicable manner. A method and system by which a true copy of a document may be stored and made accessible subsequent to its creation during an Internet-based commercial transaction would be a welcomed improvement. These and other benefits are provided in the present invention.

SUMMARY OF THE INVENTION

A method, system and pogram for ensuring the authenticity of electronic documents generated during E-commerce transactions is disclosed. The method, means and program function include the steps of (1) creating an electronic depository for storing electronic documents generated during an E-commerce transaction, (2) enabling an automatic transmittal of an electronic document to the electronic depository; and (3) storing the electronic document in the electronic depository.

Access permission to the depository is managed so that write access of the document is limited to a single initial access and subsequent access to the document is restricted to a read only access. This ensures that no changes may be made to the electronic document once it has been created and stored. The document is given a transaction identifier, which is provided to the parties to the transaction. Viewable access is provided to each party by use of this identifier.

The above as well as additional objects, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 depicts a data processing system, in which a preferred embodiment of the present invention may be implemented;

Figure 2 is a high-level block diagram of a distributed data network in accordance with one embodiment of the present invention;

Figure 3 is a high-level block diagram illustrating a client-server-depository network structure in accordance with one preferred embodiment of the present invention;

Figure 4 is a high level logical flow chart depicting the process of a preferred implementation of the present invention;

Figure 5A is a high-level block diagram illustrating a client-server-depository network structure, which ensures privacy of buyers in accordance with another preferred embodiment of the present invention;

Figure 5B is a high-level block diagram illustrating a client-server-depository network structure, which ensures privacy of buyers during purchase of an electronic product in accordance with another preferred embodiment of the present invention;

Figure 6A is a high level logical flow chart depicting the process of ensuring privacy of buyers in accordance with a preferred implementation of the present invention; and

Figure 6B is a high level logical flow chart depicting the process of ensuring privacy of buyers for electronic products in accordance with a preferred implementation of the present invention;

Figures 7A and **7B** illustrates two methods of ensuring privacy of both parties to a transaction in accordance with one embodiment of the present invention;

Figures 8A and **8B** depicts the client graphical user interface during an E-commerce transaction in accordance with one embodiment of the present invention; and

Figure 8C depicts the client graphical user interface during an E-commerce transaction where privacy of the buyer is maintained in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is directed to a method, system and program for maintaining privacy of personal information during E-commerce transactions. The invention is described with reference to a commercial transaction involving a merchant and a buyer. Use of these terms are not meant to be restrictive on the invention as other types of commercial and non-commercial transactions, which may occur on the Internet between two parties and result in the generation of an electronic document, are contemplated. For the purposes of this invention, the term merchant, seller and web site or web server are utilized interchangeably to refer to one party to a transaction, whether an individual or a corporation, who has an accessible site on the Internet at which another party may enter into a transaction. Buyer or client refers to the other party to a transaction. The term document as utilized herein may refer to a simple sales receipt or a more complex contract or agreement. Finally, all communication and transactions occur within the electronic medium (i.e., Internet) unless stated otherwise.

With reference now to the figures and in particular with reference to **Figure 1**, a data processing system that may be utilized as a buyer's terminal or server on the Internet is presented. Data processing system **20** comprises a Central Processing Unit (CPU) housed in a system unit **22**. System unit **22** also provides connections for various hardware components including disk drives **40**, and memory devices (not shown). Stored within memory devices are the operating system (OS) **24** and software

applications **26** by which many of the processes of the invention are implemented as will become clear later. Several peripheral input/output devices are connected to the CPU. These input/output devices include keyboard **82**, mouse **84**, printer **94**, CD-ROM **78**, and display monitor **30**. Display monitor **30** provides a graphical user interface (GUI) which allows a user to view and interact with software applications **26** stored in system memory or provided via a network, by displaying icons or other selectable mechanisms with which the user may interact.

Also coupled to CPU are various devices, including modem **92**, and network adapter **90**, utilized for connecting data processing system **20** to other systems and/or networks, such as is illustrated in **Figure 2.** CD-ROM **78**, modem **92**, and network adapter **90** are depicted as external components; however those skilled in the art are familiar with the various structures of data processing system architecture and understand that these components may be housed inside of system unit **22**.

Modem **92** is a communication device that enables a computer to transmit information over standard telephone lines or wireless connections such as cellular. Modem **92** converts digital computer signals to interlock signals suitable for communications over these telephone media. Modem **92** can be utilized to connect data processing system **20** to a web server via remote access protocols. Modem **92** may also provide a connection to other sources, such as an electronic bulletin board (BBS) or the World Wide Web.

Referring now to **Figure 2,** there is depicted a basic representation of a distributed data network, such as the Internet. Internet **203** is depicted as a network cloud with connections to userPC **201** (i.e. the buyer's terminal), merchant web server **205**, and depository **207**. Web server **205** is typically a data processing system having a database, OS, and server software. UserPC **201** is also typically a data processing system with OS and web browser software stored locally in memory for accessing sites on Internet **203**. UserPC **201** is utilized by a buyer to access Internet **203** and conduct transactions with web server **205.** Each node at which a connection to Internet **203** is made has a corresponding Internet Protocol (IP) address and universal resource location (URL). Communication within the Internet may be handled via Transmission Control Protocol/Internet Protocol (TCP/IP) or other transfer protocol, which allows information to be transmitted to and from addresses assigned to each node. Use of URLs, for example, are common in modern networks. For example, web server **205** is made accessible to the users of the Internet via a web address, www.merchant.com **206.** Depository **207** also has a corresponding URL, www.depository.com **208.** Those skilled in the art appreciate that Internet **203** as illustrated herein may in fact be represented as an even more complex network of servers and with multiple buyers simultaneously accessing these servers to conduct E-commerce transactions.

A. ENSURING INTEGRITY OF TRANSACTIONS

In a preferred embodiment, depository **207** is a data processing system having a data warehouse (e.g., hard drive) designed to store multiple documents **209** and provide later access to these documents **209**. The hard drive is controlled with program code which includes a file protection subroutine. The file protection subroutine provides a write-once, read-many access permission to the hard drive. Thus, millions of documents **209** generated during commercial transactions on Internet **203** may be initially written to the hard drive. Once the document **209** has been stored, it is made accessible to the transacting parties only for the purpose of reading the content. A single readable copy remains resident on the hard drive and a copy may be provided to the party who requests to view the document **209**. Although not illustrated, depository **207** may also be equipped with input mechanisms and visual output mechanism, such as a monitor, by which a depository administrator may manage the hard drive.

One preferred embodiment of the invention ensures that an E-commerce contract between buyer and seller remains unaltered after the agreement. The invention provides an electronic depository for depositing the contract after it has been created. Thus, at the conclusion of the E-commerce transaction, the contract is deposited in a third party depository via the Internet. The contract depository vouchsafes that the parties to the contract agreed to the terms of the contract. Further, the contract document cannot be modified

unilaterally because the depository is designed to not allow such alterations as described above. In case of later disputes the buyer, seller, arbitrator or judge can review the contract easily by accessing the third party depository over the Internet utilizing an assigned document identifier.

Transmittal of the contract to a depository occurs as a result of a prior selection by the seller or buyer to utilize the depository during all E-commerce transactions. In one embodiment, the depository is an independent service made available to E-commerce servers (and/or clients). The E-commerce server subscribes to the depository, and the E-commerce server's program code which handles its transactions is modified. This modification allows it to instantaneously link to the depository and transmit a document to the depository when a transaction is completed. Thus, all electronic documents generated during E-commerce transactions made on the E-commerce server are instantaneously forwarded to the depository. Alternatively, the depository may be made available for subscription by the clients who wish to protect their transactions.

The depository may be managed by a system manager. Stored documents may be time-limited (i.e., stored for only a given period of time, such as 6 months.). Each stored document is provided with a reference number or identifier (ID) by which the client and/or merchant may later access and view the document.

Turning now to **Figure 3**, there is illustrated a different representation of a client-sever-depository configuration according to a preferred embodiment. E-

commerce server **301** represents the merchant in this description. E-commerce server **301** communicates with E-commerce client (buyer) **303** via a connection over the Internet (not shown). Both components are in turn capable of communicating with depository **305**.

Figures 8A and 8B are graphical representations of a web browser utilized by a buyer during an E-commerce transaction described with reference to **Figure 4**, according to one embodiment of the invention. Web browser **800** is created with software code stored on the local client system and includes program subroutines for enabling a split screen representation as illustrated. First frame **803A** is the buyer's connecting portal to the web site of the E-commerce server. As shown in **Figure 4**, the transaction process begins at block **401** usually when the buyer connects to the E-commerce server. The buyer views the seller's merchandise/products in first frame **803A** at block **403** and enters into a transaction for the purchase of a selected item at block **405**, by interacting with E-commerce server (i.e., making selections of items displayed, etc.) in first fram **803A**. Second frame **805A** is the buyer's portal to the depository. In the preferred embodiment, when the buyer completes his transaction on first frame **803A** and selects the completion button **807** on first frame **803A**, the transaction request is sent to the E-commerce server. The server then returns a modified first frame **803B**, at block **407**, in which the transaction information is presented for buyer acceptance as shown in **Figure 8B**.

At block **409**, the buyer selects the accept button **808** in modified first frame **803B** and relevant information concerning the transaction is simultaneously transmitted to the depository at block **411** and mirrored in modified second frame **805B**. By this method, the agreement is recorded as soon as the transaction is completed. The process of **Figure 4** then ends at block **413** and the modified first frame **803B** returns to the beginning of the transaction page for a new transaction.

In a person to person transaction, both parties may have similar split-screens, so that the saved agreement is available to both parties for viewing while the transaction is being completed. The reference document number/ID is instantaneously assigned and transmitted to both parties when a document is received for storage as illustrated in second frame **805B** of **Figure 8B**. In most application of the invention, the transactions will not be person to person as the server side transactions are generally automatic (i.e., processor controlled and transacted).

B. PRIVACY OF PERSONS ENTERING INTO E-COMMERCE TRANSACTIONS

In another embodiment, the third party contract depository described above is adapted to provide enhanced privacy and security during E-commerce transactions. The depository executes registration code that stores personal "information", including financial information, and provides each subscriber with a transaction ID (TID) and password. The TID is utilized by the subscriber to

enter transactions over the Internet without revealing his/her personal information. The depository further executes transaction code by which the E-commerce transactions are completed. Limited access to the personal information is provided to the subscriber by the assigned password; however, no access is provided to the second party to a transaction except for payment information such as a credit card number. In one embodiment, the depository is controlled by the credit card company utilized in the transactions.

In traditional E-commerce transactions, products are typically sent from the merchant to the buyer using independent commercial shipping agencies (shippers) such as the United States Postal Service, United Parcel Service (UPS), Federal Express, etc. For example, many companies, which transact on-line, utilize UPS to ship their products. UPS sends its trucks to the company's physical site and picks up the products. Unlike the traditional pick-up method, where the product is labeled with the buyer's name and address, a security routing ID (SRID) is utilized in the invention. UPS is provided with a security routing ID along with the name and address of the buyer, which it places on the packages based on the SRID. In this manner, the buyer's personal information (e.g., name and address) is only placed on the product once it has reached the shipper, and the seller is never provided with this personal information.

Referring now to **Figure 5A**, a block diagram representation of a second preferred embodiment of the invention is illustrated wherein privacy of a buyer is maintained during a commercial transaction. E-Commerce client **503** is linked via the Internet to E-commerce

server **501**. Connecting arrows **502** indicate the direction of flow of information during an E-commerce transaction. Both E-commerce client **503** and E-commerce server **501** are linked to depository (database) **505**. Depository **505** is in turn linked to a shipper **507**, who is responsible for shipping the products sold by E-commerce server **501** to E-commerce client **503**. Shipper **507** delivers the products purchased during an E-commerce transaction to physical address **509** of E-commerce client **503** via physical delivery route **508**.

In another embodiment, illustrated in **Figure 5B**, an electronic product (such as downloadable software or e-books) is purchased by E-commerce client **503**. The physical delivery route **508** and physical address **509** of **Figure 5A** may not be required. Instead, connection via the Internet with the buyer's electronic (e.g., e-mail) address **504** is utilized, or alternatively, direct download to a storage location of a buyer's computer system is utilized. In **Figures 5A,** and **5B**, the numbers on the arrows show the progression of the entire transaction as discussed in **Figures 6A** and **6B** below.

Figure 6A illustrates the process by which personal information required to complete a commercial transaction is provided only to a third party (i.e., not the merchant). The process begins at block **601**. Prior to the transaction, the buyer's personal information is stored in the depository and the buyer is issued a transaction identifier (TID) at block **603**. The buyer

then accesses the merchant's web site and begins the transaction at block **605**. During the transaction, the buyer selects the method by which he wishes to identify himself, (i.e., the buyer may wish to enter all his personal information into the web site if he is not concerned with privacy and/or security or he may choose to provide only his TID if he is concerned with privacy or security). Entering of personal information tends to be time consuming and regular on-line shoppers may utilize the functionality of the invention to reduce transaction time. In the preferred method of the invention, the buyer identifies himself to the seller only by his TID at block **607**. When the transaction is completed, the E-commerce server forwards the buyer's TID to the depository at block **609**. A check is made for the TID within the depository at block **611**. If the TID is found (i.e., valid), then the transaction is approved and the buyer is sent an email or other message notifying him that his TID has been utilized at block **617**. The E-commerce server is sent the SRID number and payment (e.g., credit card number) by the depository. The depository then forwards the buyer's personal information (i.e., physical address, etc.) along with the sellers information and SRID to the shipper at block **619**. The E-commerce server alerts its warehouse/shipping personnel to prepare the product for pick-up by the shipper based on the SRID number. The SRID number is therefore provided to all parties involved (i.e., the buyer, web server, shipper and depository) to identify the transaction and related product. The process then ends at block **621**.

If the TID is not found within the depository at block **611**, the web server is notified at block **613**. The web server then declines the transaction until a correct TID is provided or the buyer provides the information required in some other way at block **615**. The process then ends at block **621**.

Although the process has been outlined utilizing the above process blocks, those skilled in the art will appreciate that other process blocks could have been included within the scope of the invention and those depicted are for illustration only. For example, process block **619** may be followed by a process block at which the shipper transmits the product (electronically or physically) to the buyer before the process ends. Also, another process block may have been included in which the depository optionally contacts, via instant messaging, the buyer to obtain verification of the transaction from the buyer.

The above process is now revisited for transactions involving electronic products (i.e., not physical products that have to be physically shipped) and with reference the **Figures 5B** and **6B**. The process begins at block **650**. The buyer places an order for an electronic product (E-product (e.g., an E-book or software)) at block **651**. Once the order is placed, an order number and price is assigned to the transaction at block **653**. The communication application of the buyer's computer system then automatically transmits the order number and price to the third party depository at block **655**. Upon receiving the transaction information, the third party

depository sends the payment amount to the E-commerce server along with the order number at block **657**. The E-commerce server transmits the E-product to the third party depository at block **659**. Finally, the third party depository transmits the E-product to the buyer at block **661**. The process then ends at block **663**. The order number is attached to each of the above electronic transmittals to track the buyer and respective seller. In one embodiment, the order number has a seller's identifying information so that it is easily found in a database lookup at the depository.

In an alternative embodiment, the server may directly send the electronic product to the buyer once payment is received at block **657**; however this permits the seller to have the buyer's email address, which may not be desired.

Figure 8C illustrates a graphical user interface (web browser) within which a user may complete an anonymous E-commerce transaction. The layout of **Figure 8C** has been described above with reference to **Figures 8A** and **8B**. Also illustrated in **Figure 8A** is a buyer information box **804** in which a buyer may elect to enter his TID number to preserve his anonymity or alternatively to enter his personal information. Once a TID number is entered, the process of utilizing the depository to complete the transaction is initiated. In **Figure 8C**, first frame **803C** has a transaction completion page displayed in which a buyer's TID is shown as having been entered. Second frame **805C** illustrates transaction information at the depository based on a transfer of an

electronic product from seller to depository utilizing the SRID number and buyer's TID number.

A more specific example is now presented. In this example, third party depository is controlled by a credit card company. The credit card company provides the service of managing the delivery of purchased products from an E-commerce transaction concluded with the buyer's issued credit card number and the TID. The buyer provides the credit card company with his e-mail address and/or physical mailing address when he obtains the credit card and corresponding card number. When the buyer buys from an electronic merchant, he provides the merchant with only his TID number. In case of a purchase of an electronic product, the merchant sends the electronic product with the TID number to the credit card company and the credit card company forwards the electronic content to the buyer and the required payment to the merchant.

In case of physical delivery of merchandise to a physical address, the merchant sends to the credit card company (1) the TID number, (2) the corresponding SRID number (which could be the same as the credit card transaction authorization confirmation number received from the credit card company), and (3) the name of the shipping agent. The credit card company links the address field for the buyer and the corresponding SRID number and forward these to the shipping agent.

The merchant provides the SRID number on the package to be delivered, and the shipping agent attaches the physical address obtained from the credit card company. Hence, the seller is never provided with the buyer's

shipping address (or name), thereby ensuring anonymity. This process also ensures that the package is shipped only to the buyer's shipping address provided to the credit card company, which allows for added security. Accordingly, privacy of the buyer is substantially improved and/or maintained with the exception of his credit card number. Security is enhanced as the credit card issuer can ensure that the product is delivered to the appropriate person and the appropriate physical or electronic address.

An extension of the above embodiment operates to provide a 2-party anonymous transaction (i.e., both parties maintain confidentiality). In **Figure 7A**, client A **701** and client Z **703** are each assigned a unique TID, X and Y, respectively. The unique TID is linked within the depository **705** to the user's name, e-mail address, physical address and credit card number. Depository **705** is utilized as a transaction proxy. Client A **701** advertises merchandise on depository **705** with his TID. Client Z **703** substantially may access the depository **705** and purchase the merchandise utilizing his TID. The depository **705** forwards the payment to client A **701** and ships the product to client Z **703**.

Figure 7B illustrates the use of the third party depository **709** as a proxy server. Use of the third party depository **709** as a proxy server operates to protect the personal information of both the seller web server, client A **707** as well as the buyer, client Z **711**. Thus each party is assigned a pseudonym or TID and transact

through the depository via the pseudonyms. In this way, client z **711** does not have access to the name and address of the owner of the server **707** via the server databases established by Network Solutions, for example.

Some of the advantages of the use of a third party depository include:

1. The use of a depository is much more understandable to unsophisticated users as it does not involve digital signatures, which are complex and prone to fraud;

2. The use of a depository eliminates the associated overhead and recurring yearly costs of certifying digital signatures, which is high for individual buyers;

3. Storage of a contract in a third party depository (particularly if it is for a few months for a merchandise purchase) is very cheap as disk space is inexpensive; and

4. In contested transactions, a single sheet agreement on terms and price that is maintained in a third party depository is very beneficial in establishing the true terms of the agreement.

It is important to note that while the present invention has been described in the context of a fully functional data processing system, those skilled in the art will appreciate that certain elements of the method of the present invention are capable of being distributed in the form of a computer readable medium of instructions

in a variety of forms, and that the present invention applies equally, regardless of the particular type of signal bearing media utilized to actually carry out the distribution. Examples of computer readable media include: nonvolatile, hard-coded type media such as Read Only Memories (ROMs) or Erasable, Electrically Programmable Read Only Memories (EEPROMs), recordable type media such as floppy disks, hard disk drives and CD-ROMs, and transmission type media such as digital and analog communication links.

While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention. For example, although the invention has been explained with reference to protecting the personal information of the buying party, it is conceivable that the invention may be applied to transactions where the selling party desires his personal information be protected.

CLAIMS:

What is claimed is:

1. A method for ensuring the authenticity of electronic documents generated during E-commerce transactions, said method comprising the steps of:

enabling automatic transmittal of an electronic document to an electronic depository in response to a completion of an E-commerce transaction in which said electronic document is created; and

storing said electronic document in said electronic depository.

2. The method of Claim 1, wherein said storing step further includes the steps of:

generating a document ID for said electronic document; and

providing said document ID within a confirmation receipt to each party of said E-commerce transaction.

3. The method of Claim 1, wherein said electronic document is a contract between a buyer and merchant entered into on a web server of said merchant and said enabling step includes the steps of:

transferring an electronic document when said document is created during an E-commerce transaction; and

linking said modified web server to said depository.

4. The method of Claim 1, wherein said enabling step further includes the step of utilizing a web browser application of a buyer to create a link to said depository when said buyer enters into an E-commerce transaction.

5. An electronic database used as a depository for electronic documents generated during E-commerce transactions, comprising:

means for automatically receiving an electronic document after an E-commerce transaction has completed;

means for generating a document ID for said received E-commerce document; and

means for storing said electronic document.

6. The electronic database of Claim 5, wherein said means for generating said document ID further includes means for transmitting said document ID to each party to said E-commerce transaction, which produced said electronic document.

7. The electronic database of Claim 5, wherein said means for storing further comprises:

means for allowing a later read access to said E-commerce document by a party to said E-commerce transaction; and

means for preventing modifications to said E-commerce document after it has been stored.

8. A computer program product for ensuring authenticity of electronic documents generated during E-commerce transactions, comprising:

a computer readable storage medium; and

program instructions on said computer readable storage medium for:

connecting an Internet client to an electronic depository and a merchant web server;

displaying an E-commerce transaction between said Internet client and said merchant web server via a graphical user interface of said Internet client;

automatically forwarding to said electronic depository a copy of an electronic document generated during said E-commerce transaction.

9. The computer program product of Claim 8, further including program instructions for:

tagging said electronic document with a read and write access, wherein said electronic document is stored at said depository in a write-once, read-many format;

generating a document identifier (ID) to identify said electronic document; and

allowing later retrieval of said electronic document utilizing said document ID.

10. The computer program product of Claim 9, wherein said program instructions for generating said document ID includes program instructions for transmitting said document ID to the other party to said E-commerce transaction and to said depository.

11. A depository for ensuring the authenticity of electronic documents generated during E-commerce transactions, said depository comprising:

means for enabling automatic receipt of an electronic document, in response to a completion of an E-commerce transaction in which said electronic document is created; and

means for storing said electronic document in said electronic depository.

12. The depository of Claim 11, wherein said storing means includes:

means for limiting a write access of said electronic document to a first access; and

means for restricting subsequent access to said document to read-only access, such that no changes may be made to said electronic document once it has been stored.

13. The depository of Claim 11, further including:

means for controlling a read and write access to said electronic depository, wherein said document is stored in a write-once, read-many format;

means for generating a document identifier (ID), to identify said electronic document; and

means for later retrieving said electronic document for a party to said E-commerce transaction.

14. The depository of Claim 13 wherein said controlling means further includes:

means for enabling a non-modification function for said electronic document, wherein a control code of said electronic depository is activated to prevent later modification to said electronic document; and

means for flagging electronic document within said electronic depository to allow a later read access to said E-commerce document by a party to said E-commerce transaction.

15. A computer program product for ensuring the authenticity of electronic documents generated during E-commerce transactions, said program product comprising:

a computer readable medium; and

program instructions stored on said computer readable medium, including:

program means for enabling automatic receipt of an electronic document, in response to a completion of an E-commerce transaction in which said electronic document is created; and

program means for storing said electronic document in said electronic depository.

16. The computer program product of Claim 15, wherein said storing means includes:

program means for limiting a write access of said electronic document to a first access; and

program means for restricting subsequent access to said document to read-only access, such that no changes may be made to said electronic document once it has been stored.

17. The computer program product of Claim 15, further including:

program means for controlling a read and write access to said electronic depository, wherein said document is stored in a write-once, read-many format;

program means for generating a document identifier (ID), to identify said electronic document; and

program means for later retrieving said electronic document for a party to said E-commerce transaction.

18. The computer program product of Claim 17 wherein said controlling means further includes:

program means for enabling a non-modification function for said electronic document, wherein a control code of said electronic depository is activated to prevent later modification to said electronic document; and

program means for flagging electronic document within said electronic depository to allow a later read access to said E-commerce document by a party to said E-commerce transaction.

ABSTRACT OF THE DISCLOSURE

THIRD PARTY CONTRACT DEPOSITORY FOR E-COMMERCE TRANSACTIONS

A method, system and program for ensuring the authenticity of electronic documents generated during E-commerce transactions. The method, means and program function include: (1) creating an electronic depository for storing electronic documents generated during an E-commerce transaction, (2) enabling an automatic receipt at the electronic depository of an electronic document created during an E-commerce transaction; (3) storing the electronic document in the electronic depository; (4) providing each party to the transaction with a document ID for later access to the electronic document; and (5) allowing later read-only access to the electronic document and preventing any modifications to the document once it has been stored.

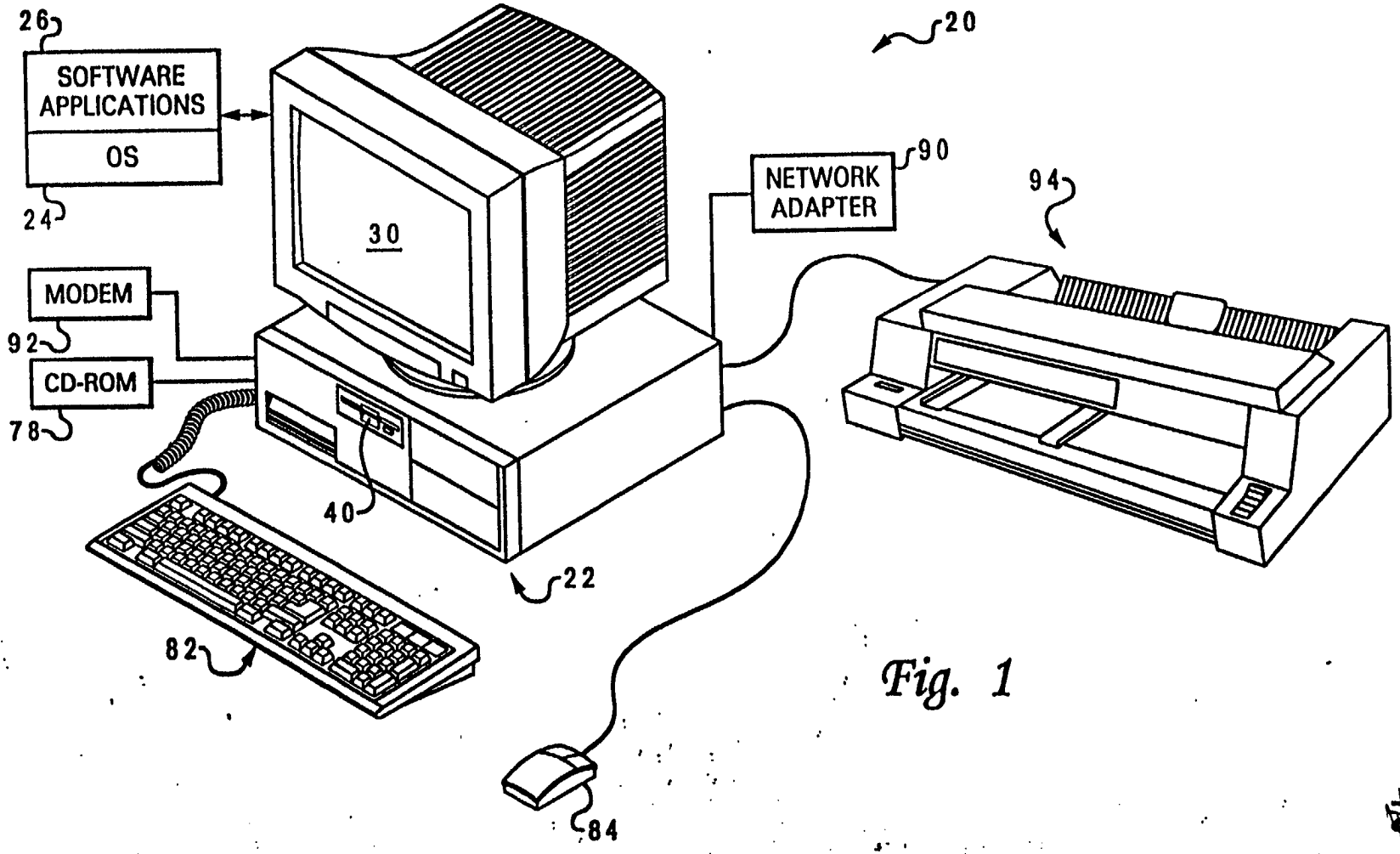


Fig. 1

09535550 .032700

FIG 2

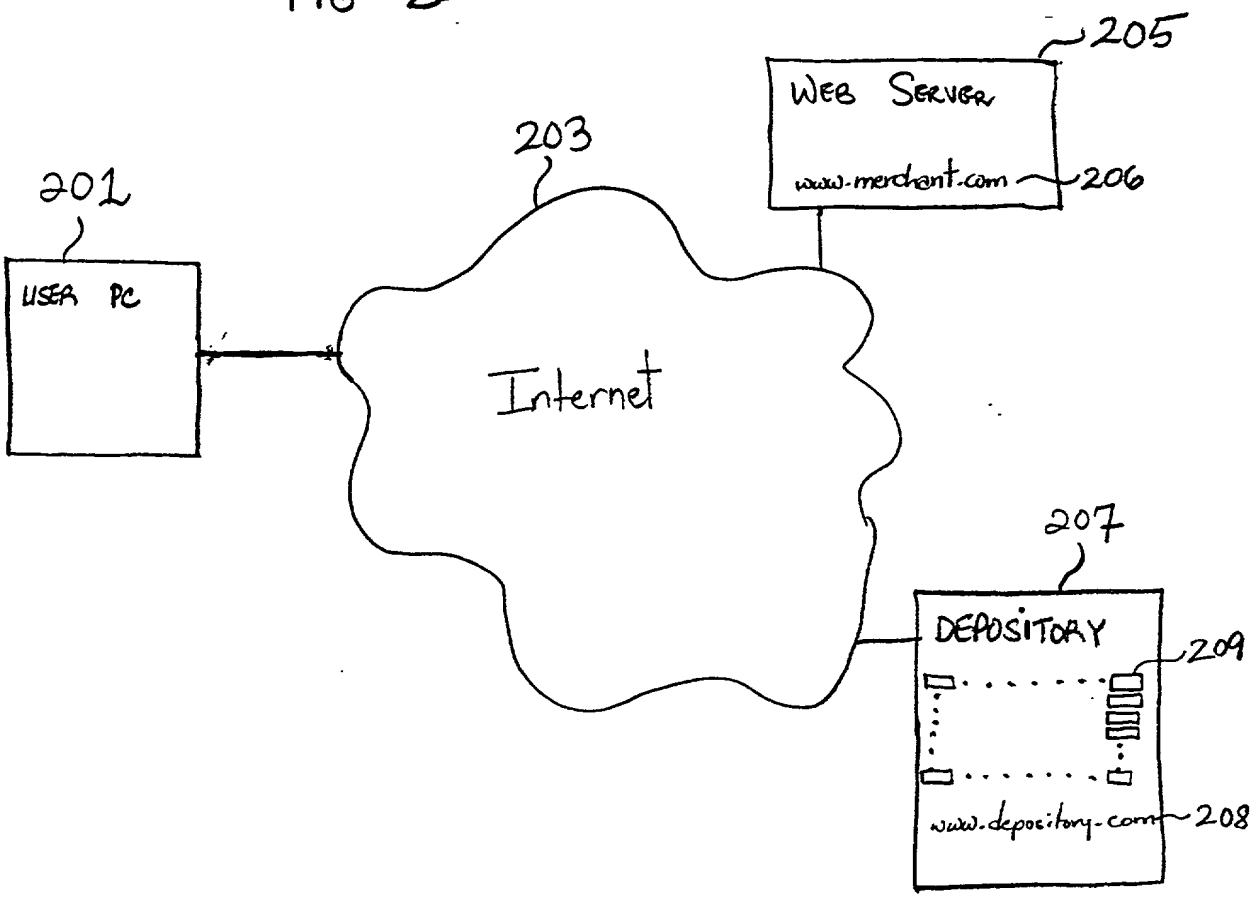
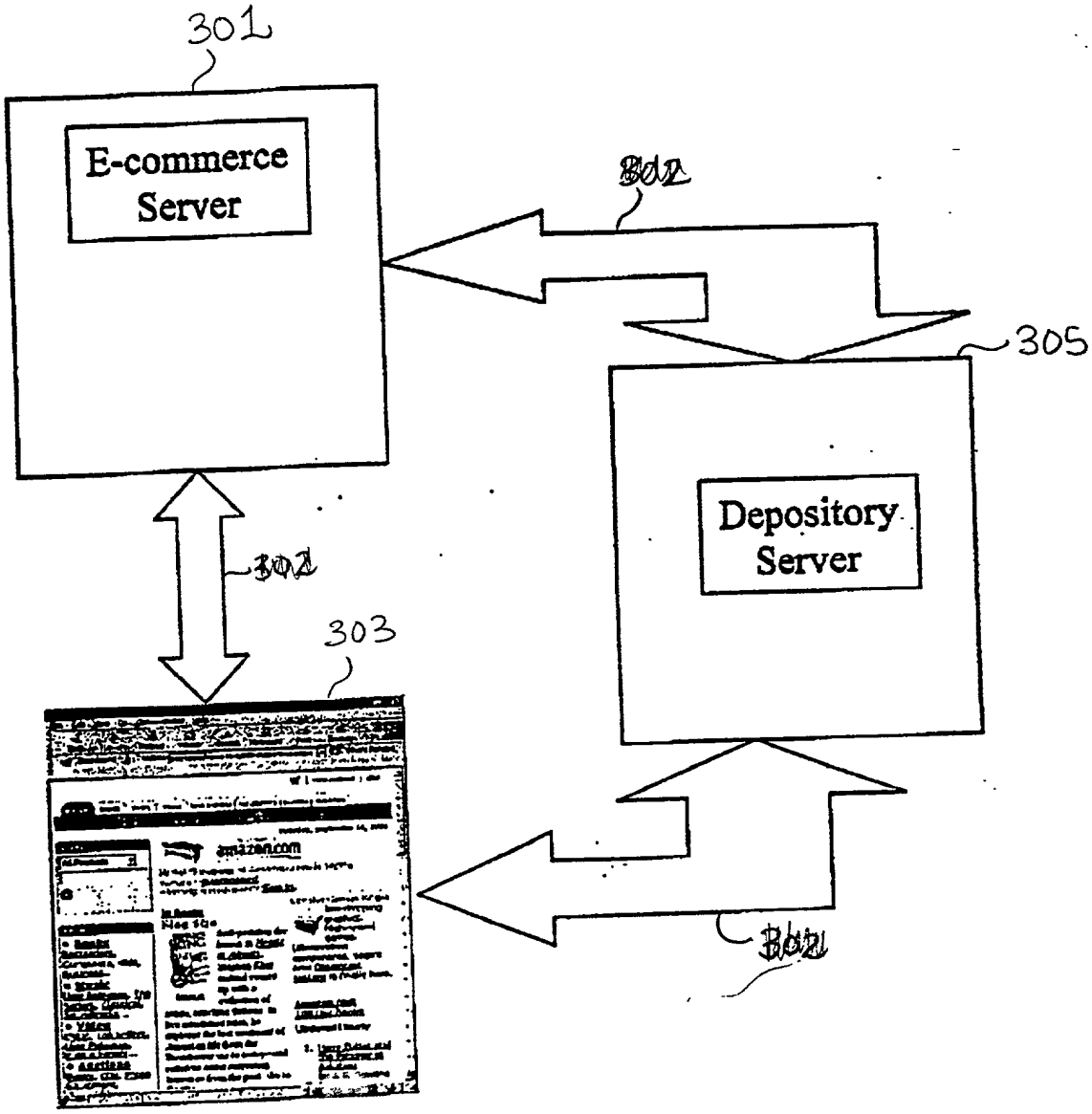
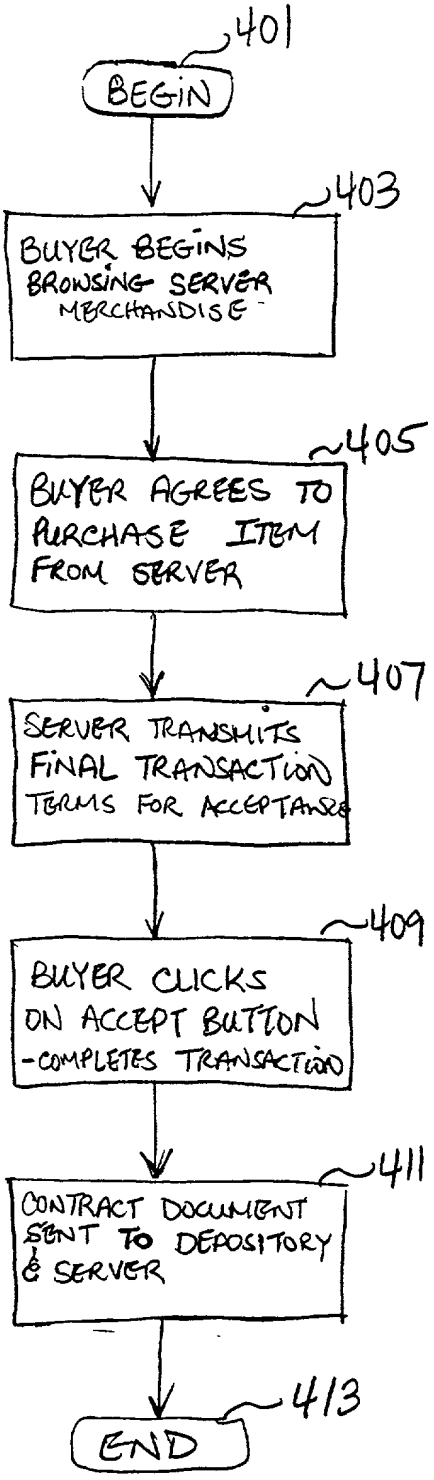

205
WEB SERVER
www.merchant.com
206
203
201
USER PC
Internet
207
DEPOSITORY
209
www.depository.com
208

Figure 3



E-commerce Client



DOCSOFT - DOCSOFT

FIGURE 5A

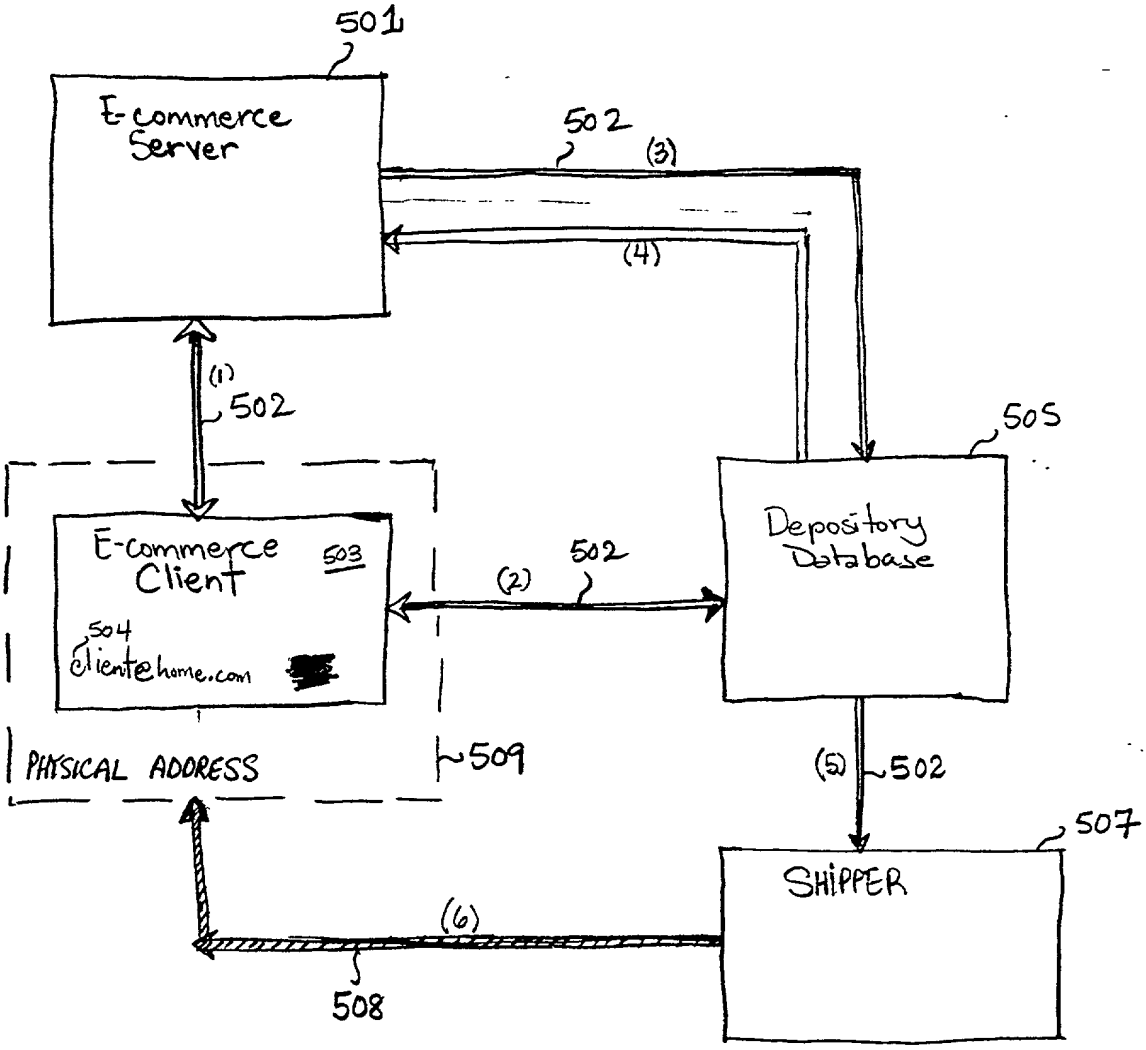
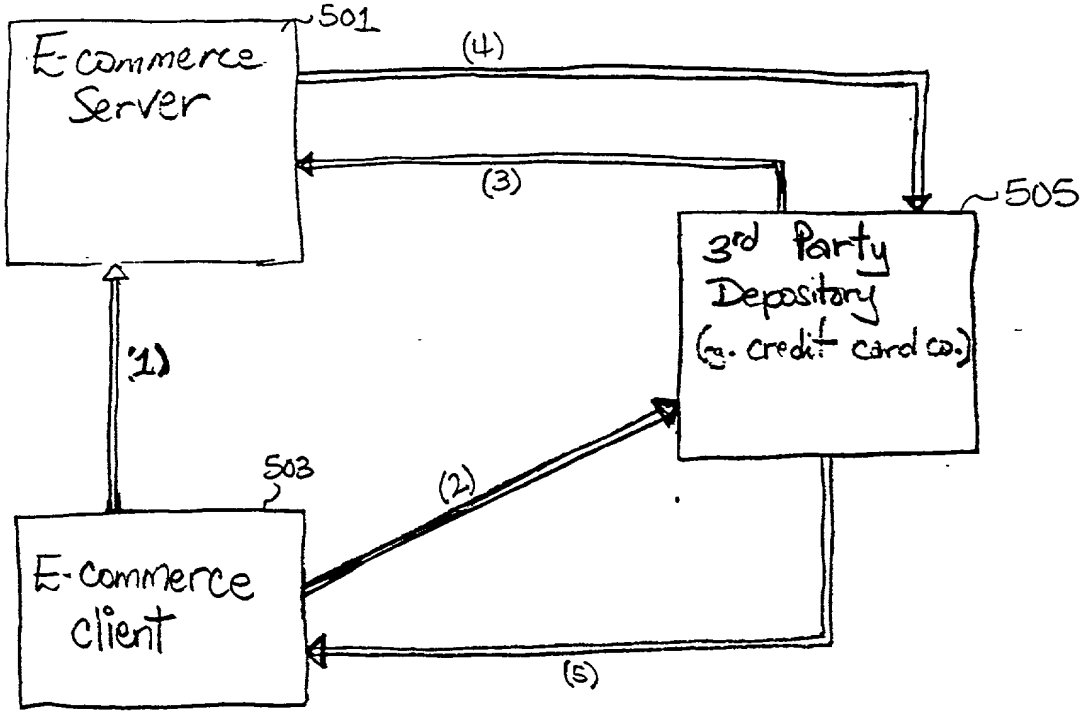

501
E-commerce Server
502
(3)
(4)
(1)
502
505
E-commerce Client
503
504
clientehome.com
(2)
502
Depository Database
PHYSICAL ADDRESS
509
(5)
502
507
SHIPPER
(6)
508

FIG 5B



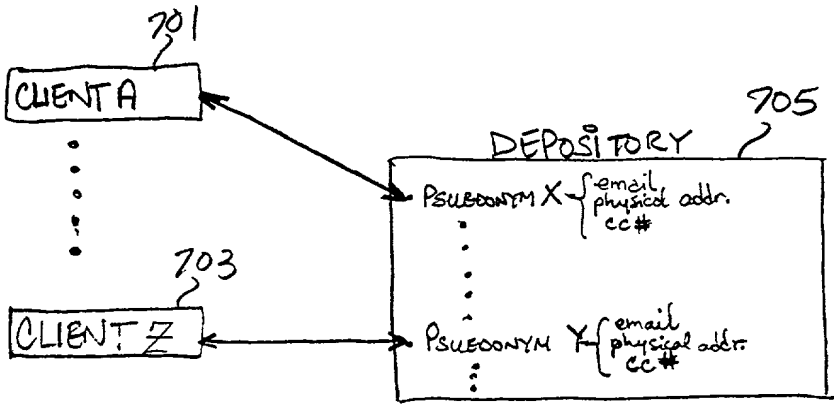


FIG 7A

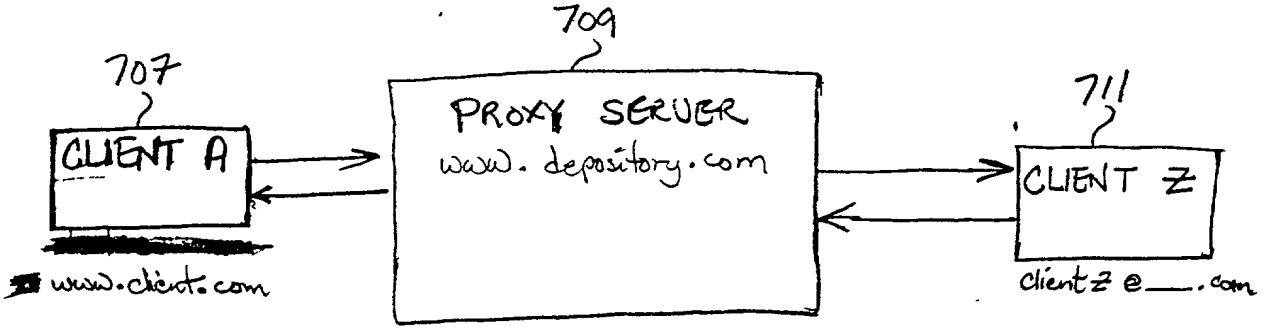


FIG 7B

FIG. 6A

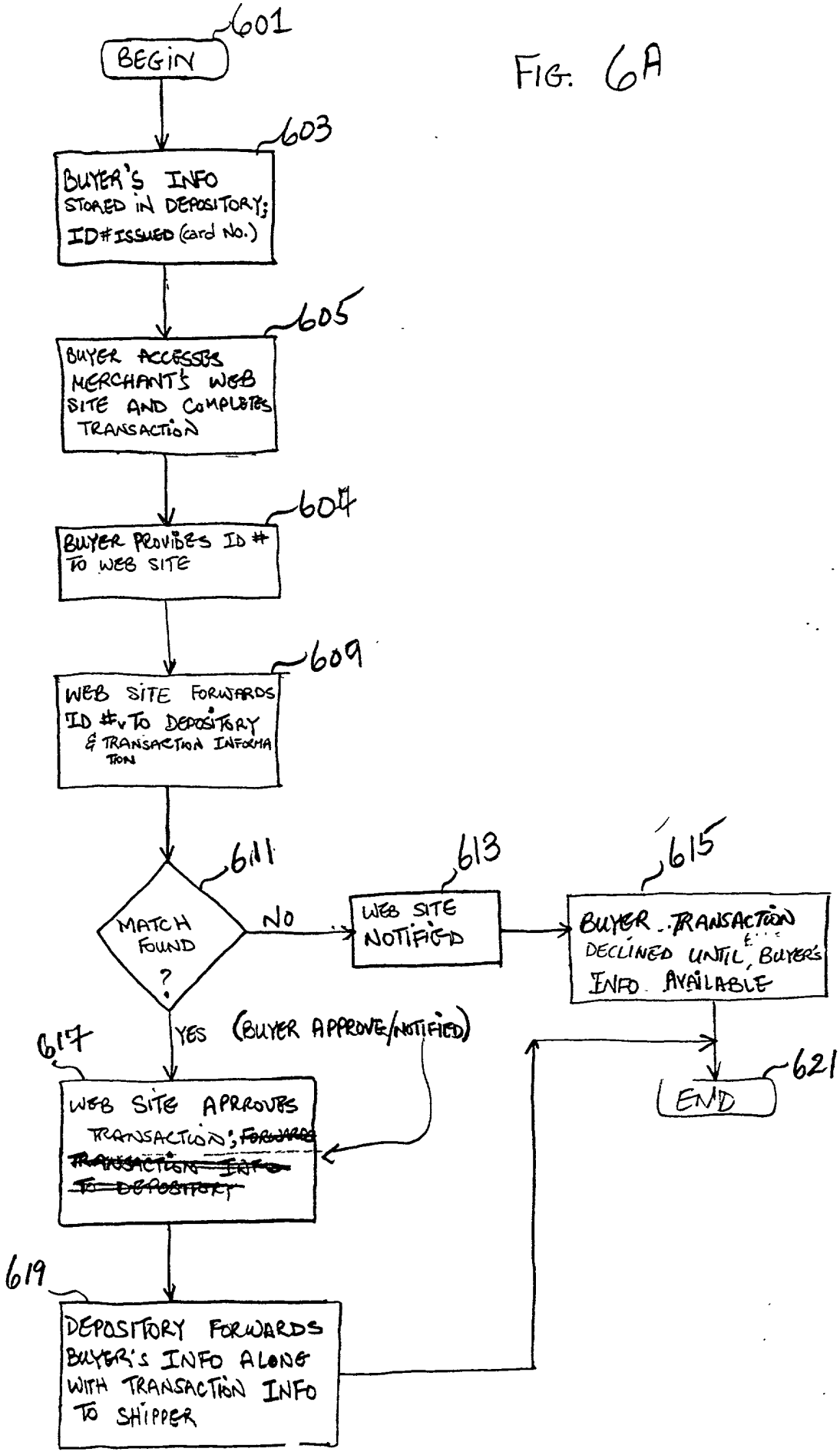
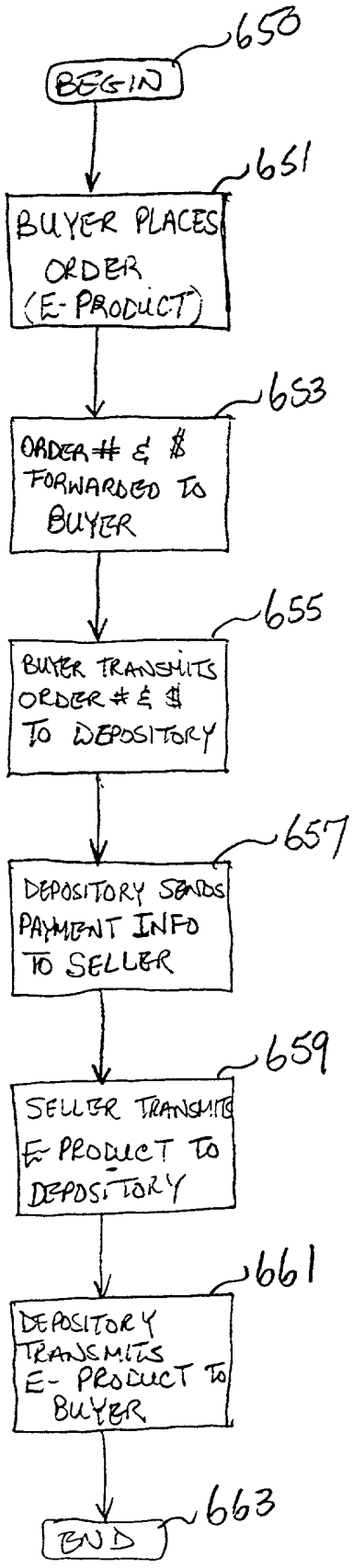

601
BEGIN
603
BUYER'S INFO STORED IN DEPOSITORY; ID# ISSUED (card No.)
605
BUYER ACCESSES MERCHANT'S WEB SITE AND COMPLETES TRANSACTION
607
BUYER PROVIDES ID # TO WEB SITE
609
WEB SITE FORWARDS ID #, TO DEPOSITORY & TRANSACTION INFORMATION
611
MATCH FOUND ?
NO
613
WEB SITE NOTIFIED
615
BUYER TRANSACTION DECLINED UNTIL BUYER'S INFO AVAILABLE
YES (BUYER APPROVE/NOTIFIED)
617
WEB SITE APPROVES TRANSACTION; FORWARDS TRANSACTION INFO TO DEPOSITORY
619
DEPOSITORY FORWARDS BUYER'S INFO ALONG WITH TRANSACTION INFO TO SHIPPER
621
END

FIG. 6B


650
BEGIN
651
BUYER PLACES ORDER (E-PRODUCT)
653
ORDER # & $ FORWARDED TO BUYER
655
BUYER TRANSMITS ORDER # & $ TO DEPOSITORY
657
DEPOSITORY SENDS PAYMENT INFO TO SELLER
659
SELLER TRANSMITS E-PRODUCT TO DEPOSITORY
661
DEPOSITORY TRANSMITS E-PRODUCT TO BUYER
663
END

800

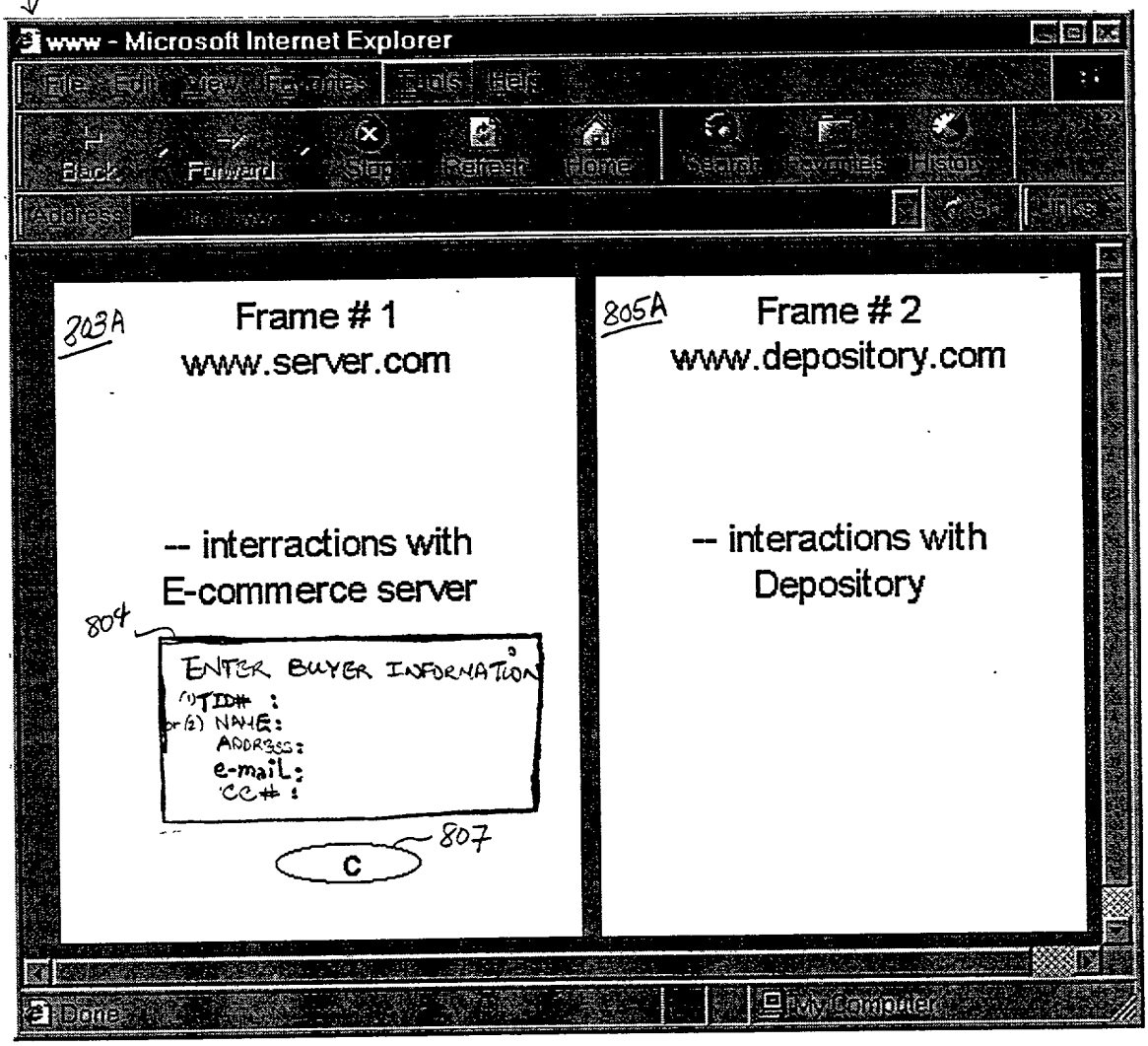


FIGURE 8A

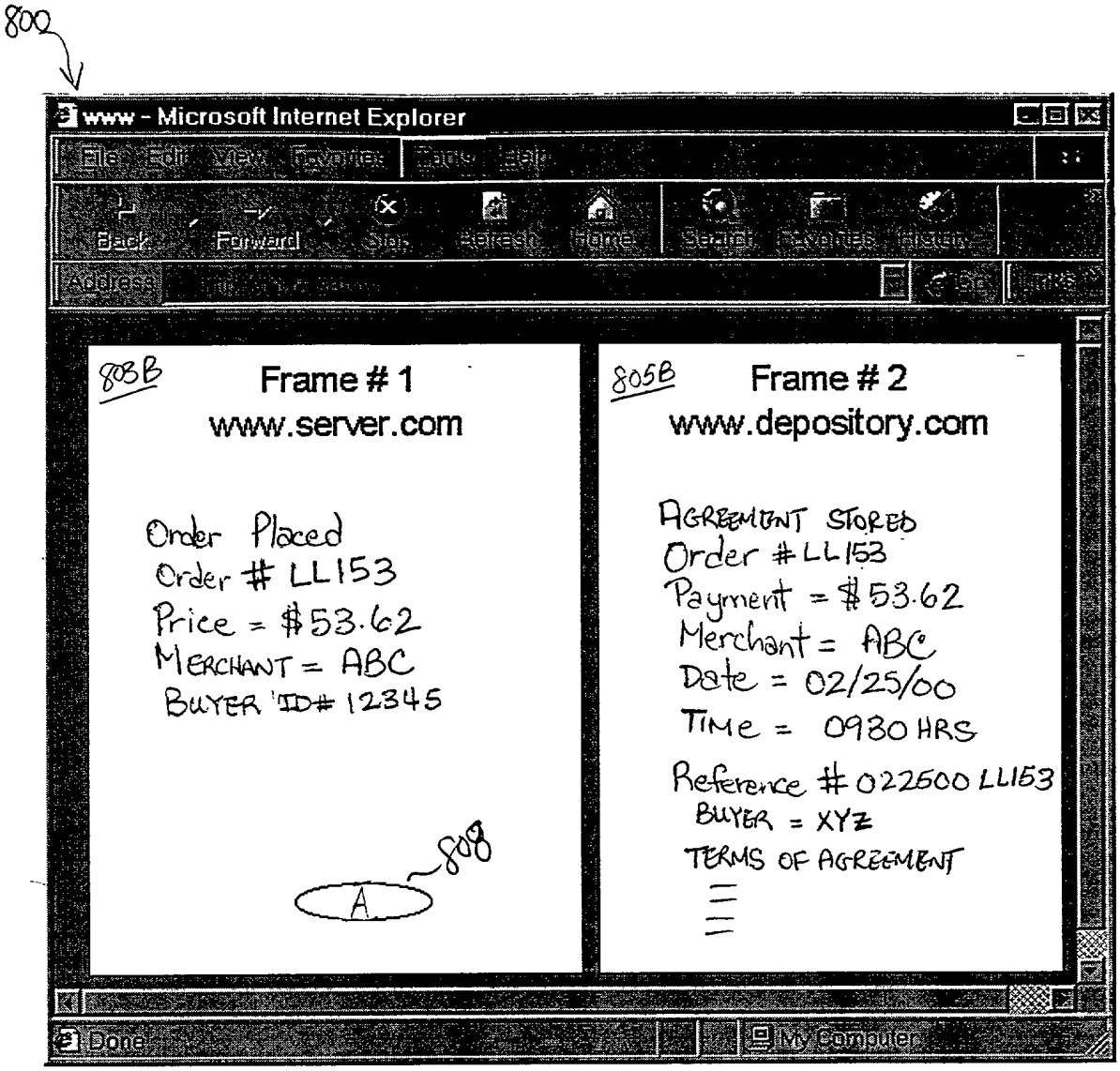


FIGURE 8B

09/25/2000 - 25555.0

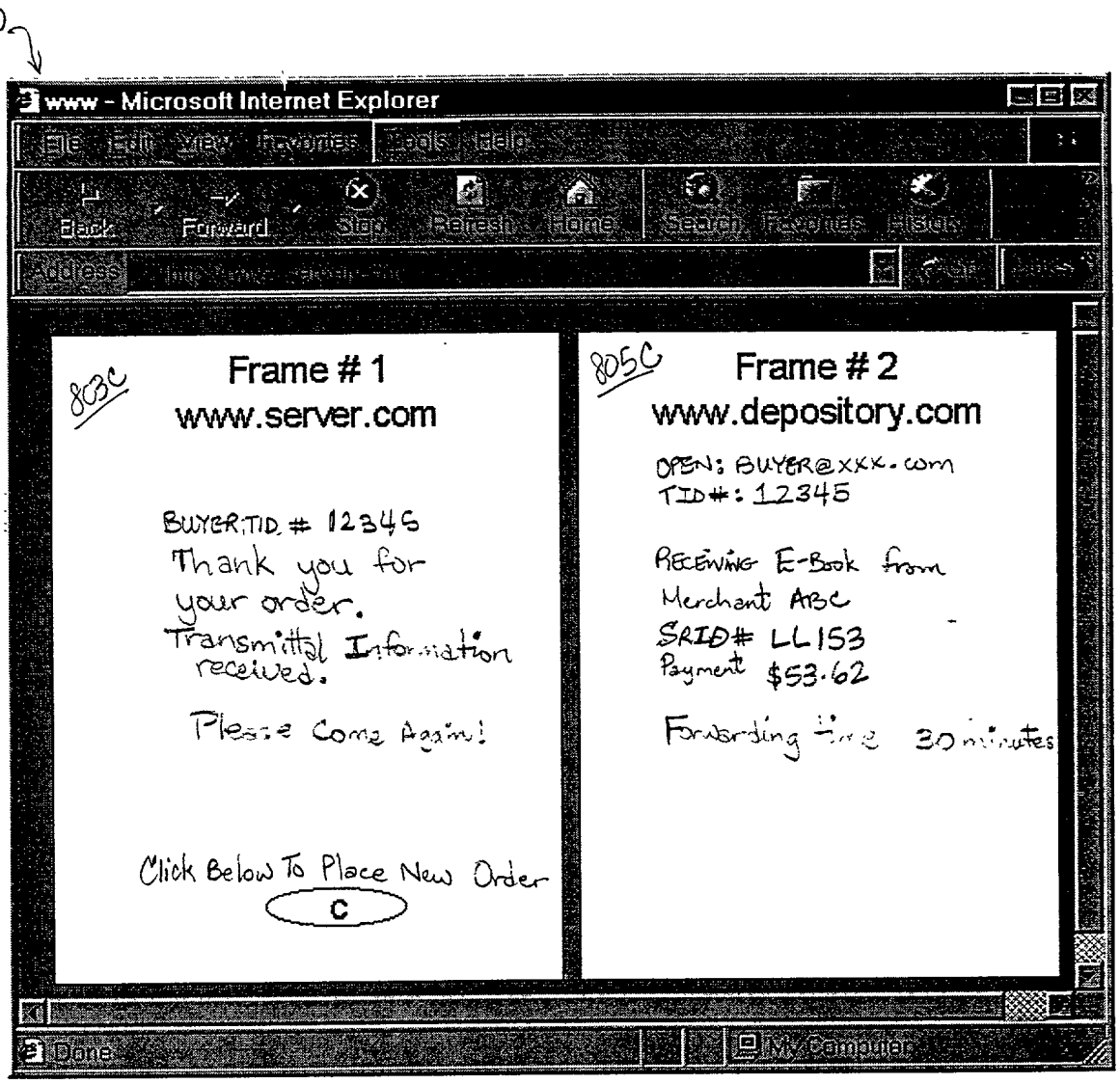


FIG 8C

0052520 - 0555550

DOCKET NUMBER: **AUS000060US1**

DECLARATION AND POWER OF ATTORNEY FOR

PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

THIRD PARTY CONTRACT DEPOSITORY FOR E-COMMERCE TRANSACTIONS

the specification of which (check one)

X is attached hereto.

__ was filed on _____
as Application Serial No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):			Priority Claimed
_____	_____	_____	___ Yes___ No
(Number)	(Country)	(Day/Month/Year)	

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information

of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial #)	(Filing Date)	(Status)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

John W. Henderson, Jr., Reg. No. 26,907; Thomas E. Tyson, Reg. No. 28,543; Robert M. Carwell, Reg. No. 28,499; Jeffrey S. LaBaw, Reg. No. 31,633; Douglas H. Lefeve, Reg. No. 26,193; Casimer K. Salys, Reg. No. 28,900; David A. Mims, Jr., Reg. No. 32,708; Volel Emile, Reg. No. 39,969; James H. Barksdale, Jr. Reg. No. 24,091; Anthony V. England, Reg. No. 35,129; Leslie A. Van Leeuwen, Reg. No. 42,196; Marilyn S. Dawkins, Reg. No. 31,140; Mark E. McBurney, Reg. No. 33114; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond, Jr., Reg. No. 18,753; Matthew S. Anderson, Reg. No. 39,093; Matthew W. Baca, Reg. No. 42,277; Michael R. Barré, Reg. No. 44,023; Max Ciccarelli, Reg. No. 39,454; Andrew J. Dillon, Reg. No. 29,634; Justin M. Dillon, Reg. No. 42,486; John G. Graham, Reg. No. 19,563; Andrew M. Harris, Reg. No. 42,638; Steven Lin, Reg. No. 35,250; Richard N. McCain, Reg. No. 43,785; Jack V. Musgrove, Reg. No. 31,986; Antony P. Ng, Reg. No. 43,427; Michael E. Noe, Jr., Reg. No. 44,975; Brian F. Russell, Reg. No. 40,796; and Daniel E. Venglarik, Reg. No. 39,409.

Send correspondence to: Andrew J. Dillon, FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP, Suite 350 Lakewood on the Park, 7600B North Capital of Texas Highway, Austin, Texas 78731, and direct all telephone calls to Andrew J. Dillon, (512) 343-6116.

FULL NAME OF SOLE OR FIRST INVENTOR: RABINDRANATH DUTTA

INVENTORS SIGNATURE: Rabindranath Dutta DATE: 3/14/2000

RESIDENCE: 3401 Parmer Lane W. #835
Austin, Texas 78727

CITIZENSHIP: India

POST OFFICE ADDRESS: 3401 Parmer Lane W. #835
Austin, Texas 78727